THE STATE OF THE SCIENCE OF SYSTEM SAFETY IN THE DEPARTMENT OF DEFENSE

Raymond S. Banas

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE STATE OF THE SCIENCE
OF
SYSTEM SAFETY IN THE DEPARTMENT OF DEFENSE

Raymond S. Banas

September 1977

Thesis Advisors: J. W. Creighton
L. E. Waldeisen

Prepared for:
Naval Air Systems Command
Washington, D.C.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NPS-54Cf 78041	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) THE STATE OF THE SCIENCE OF SYSTEM SAFETY IN THE DEPARTMENT OF DEFENSE		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis: September 1977 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Raymond S. Banas		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Project Number 56880
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE September 1977 13. NUMBER OF PAGES 68
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The possibility that the System Safety discipline, as practiced by the Department of Defense and particularly the Naval Air Systems Command (NAVAIRSYSCOM), acts as a significant barrier to the utilization of System Safety technology in the acquisition process is analyzed. Specific areas including contracting procedures, contracting documentation, specifications, regulations

and administrative procedures are investigated. Emphasis is placed on improving the effectiveness of the safety program within the Navy.

The State of the Science of System Safety in the Department of Defense

by

Raymond S. Banas
B.S. in Mechanical Engineering, 1954
M.S. in Systems Management, 1974
P.E. in System Safety, 1977

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1977

ABSTRACT

The possibility that the System Safety discipline, as practiced by the Department of Defense and particularly the Naval Air Systems Command (NAVAIRSYSCOM), acts as a significant barrier to the utilization of System Safety technology in the acquisition process is analyzed. Specific areas including contracting procedures, contracting documentation, specifications, regulations and administrative procedures are investigated. Emphasis is placed on improving the effectiveness of the safety program within the Navy.

EXECUTIVE SUMMARY

The objective of this thesis is to demonstrate that a number of serious barriers exist which preclude the utilization of an effective System Safety technology in the Department of Defense, particularly within the Naval Air Systems Command (NAVAIRSYSCOM).

Roughly, the System Safety discipline is but a decade old. A lengthy tri-service military specification describes and directs its implementation. Starting with the Air Force, the Army and Navy, in turn implemented its use. Each service, more-or-less, went its own way in interpreting how the program was to be exercised inasmuch as DOD guidance was either minimal or nonexistent. Consequently, each service and the other agencies have differences in contracting procedures, contracting documentation, specifications, regulations, and administrative procedures.

Contractors were interviewed to determine on a comparative basis just where the NAVAIRSYSCOM ranked in terms of overall performance. Results were not complimentary to the Navy. Air Force and Navy safety organizations and, to a limited degree, Army organizations were visited to ascertain operating differences.

A number of barriers were enumerated for DOD organizations and are listed in Chapter V.A., Conclusions. For the NAVAIRSYSCOM, it was found that the safety office lacked support outside of its own office and that it failed to

provide sufficient instruction within all directives dealing with contractual and project management matters. It also failed to enforce current project charters which assign "Safety Principals" to be responsive to safety matters. The NAVAIRSYSCOM also failed to provide the instructional matter, guides, manuals, etc., to accomplish the safety assignment.

TABLE OF CONTENTS

I. INTRODUCTION

The first aerospace accident was the mythological fall of Icarus. He flew too close to the sun so that the beeswax which held his wing feathers together melted. He then plunged into the ocean and drowned. (1)

Assuming some poetic license, Daedalus, father of Icarus, had performed a number of tasks to assure a successful first flight. He had inspected all feathers, all wax and all other materials used under his Quality Control Program. He had selected the right feather sizes and had them assembled in the proper places to assure reliable performance. He had done one other thing under his System Safety Program: Daedalus had performed a "Hazard Analysis" and had subsequently warned Icarus of his findings, i.e., to fly a middle course, neither too low (where moisture would increase his weight unbearably) nor too high (where the sun's heat would melt the beeswax).

Unlike the mythological flight described above, man in his infinite wisdom succeeded in finding ways to break his bond from land and soar to great heights, over great distances at high speeds. As with many other innovations pursued expressly for the betterment of man, flying machines and other equally ingenious devices have also been adapted for the destruction of man. Unfortunately, history tells us, destructive machines used against intended enemy victims

are likewise destructive to their owners, users, operators and unintended victims through accident.

At present, the federal government is supporting a number of systems safety programs on a number of projects in several agencies and departments. Current examples include the Air Bag (Department of Transportation), the ill-fated B-1 Bomber (Air Force), the Cruise Missile (Navy), and the Space Shuttle (NASA).

It is very difficult to measure their effectiveness. In short, there is a need to determine what constitutes an effective System Safety Program; what tasks must one do to assume that the system safety portion of any given project is successful, productive.

A. BACKGROUND

The first formal application of production techniques began in the 1800's. Quality Control was a fully recognized discipline in the early 1900's. Reliability came into range roughly in the 1930's, followed by Maintainability in the 1940's, and Value Engineering in the late 1950's.

The first formal mention of a discipline called "System Safety" did not appear until 1961. At this time, Air Force General Blanchard provided a keynote address to a USAF Commanders Conference. Shortly thereafter, the "Minuteman" project became the first Department of Defense (DOD) project which incorporated a requirement to perform contractually binding system safety program tasks. The contract included

a System Safety Program Specification (MIL-S-38130), a System Safety Program Statement of Work, and deliverable safety data items.

In turn, the Army and Navy members of the Defense Department followed suit. The Navy's first contractual safety application occurred in 1969 within the F-14 contract awarded to Grumman Aerospace, Inc., Bethpage Long Island, by the Naval Air Systems Command (NAVAIRSYSCOM). That year, safety requirements were subsequently included in the S-3A Aircraft award to Lockheed and the JIFDATS (Joint In-Flight Data Transmission System) award to Northrop Corporation. Figure 1 shows which projects considered a contractual safety effort, and for the years shown, illustrates rapid growth.

"System Safety" represents the next youngest discipline in the NAVAIRSYSCOM, "Survivability" being the youngest. Nevertheless, it is not so young (almost 10 years old) that barriers preventing efficient implementation should not be readily uncovered; explored and dealt with.

B. OBJECTIVE

The objective of any System Safety Program is to prevent accidents and conserve resources. The objectives of this thesis are to demonstrate that a number of barriers exist which preclude the utilization of an effective System Safety technology, and show that these problems represent a significant barrier particularly within the NAVAIRSYSCOM acquisition process.

NAVAIR PROJECTS WITH SYSTEM SAFETY INPUTS

1967-68 & Earlier	1969	1970	1971	1972	1973	1974	1975	1976
0	3	10	13	20	26	30	42	43
	F-14	F-14	F-14	F-14	F-14A/B	F-14A/B	F-14A	F-14A
	S-3A	S-3A	S-3A	S-3A	F-14H-H	S-3A COD	S-3A COD	US-3A
	JIFDATS	JIFDATS	JIFDATS	F401	S-3A	S-3A	S-3A	S-3A
		UHIN	UHIN	TACOMO	F401	PHOENIX	PHOENIX	PHOENIX
		BULLDOG	F401	PHOENIX	PHOENIX	HARPOON	HARPOON	HARPOON
		TACOMO	TACOMO	HARPOON	HARPOON	ITCS	ITCS	ITCS
		PHOENIX	PHOENIX	J402	J402	BQM34E	BQM34E	BQM34E-F
		HARPOON	HARPOON	E2C	E2C	E2C	E2C	E2C
		HLM	E2C	SIIIS3	SIIIS3	F-18	F-18	F-18
		LAMPS	SIIIS3	CH53E	CH53E	CH53E	CH53E	CH53E
			CH53	ACMR	BQM34E	AIM-9L	AQM37B	AQM37B
			ACMR	ZBQM90A	ZBQM90A	HARM	F404	F404
			ZBQM90A	AIM9L	AIM9L	IRDS	AIM9L	AIM9L
				CONDOR	CONDOR	TRAM	GATOR	GATOR
				HARM	HARM	F401	HARM	HARM
				PAVEKNIFE	PAVEKNIFE	E2 PROP	FAE	FAE II
				AGILE	AGILE	LAMPS III	IRDS	IRDS
				V/STOL	TRAM	A7E	IWDS	IWDS
				TRAM	E2 PROP	T-34C	TRAM	TRAM
				E2 PROP	LAMPS III	CMGS E-SYS	F401	F401
					CGSE	CMGS MDAC	E2 PROP	SEQ F100
					A7E	CM - G D	LAMPS III	LAMPS III
					VFX	CM - LTV	A7F	A7E
					VTP(T-34)	XFV-12A	T-34C	T-34C
					XFV-12A	HST(RAST)	CMGS E-SYS	ADEN
					CRUISE M	AV-8B	CMGS MDAC	TOMHK GS
						TACNAV	CM - G D	TOMHK
						TACOMO	CM - LTV	QSM
						TAU-3	HST(RAST)	RAST
						ULAIDS	AV-8B	AV8B
							TACNAV	TACNAV
							TACOMO	TACOMO
							TAU-3	RPV
							ULAIDS	ULAIDS
							VTAM(X)	VTAM(X)
							AN/ARC-175(V)	LUU2B/B
							AN/ARS-3	AN/ARS 3
							AN/ARN-99V	AN/ARN-99V
							AN/URN-( )	AN/ASN-124
							AN/ASN-124	AN/URN-( )
							GPU-2/A	GPU-2/A
							SM-696/ZPT	EN 126(1)
								SLU/FAE

Figure 1.

C. METHODOLOGY

The major source of data used as a primary basis for analysis was obtained through personal interviews conducted by the author.

Thirteen personal interviews were conducted at five major corporations. Three individuals were safety department heads, the balance were practicing safety engineers. The interviewees included members from Air Research Corp., Tucson, Arizona; General Dynamics, San Diego, California; Grumman Aerospace Corp., Bethpage, Long Island, New York; Hughes Aircraft, Culver City, California; and Rohr, San Diego, California.

One telephone interview and eleven personal interviews were held with safety members from five Department of Defense organizations. These were: Army Headquarters Safety Office, Washington, D.C.; the Naval Air Systems Command, Washington, D.C.; the Air Force Safety Center, Norton AFB; the Air Force Space and Missile Systems Organization (SAMSO), Los Angeles, California; and the Navy Safety Center, Norfolk, Virginia (telephone interview).

Additionally, interviews were held with members from respective Army, Navy and Air Force Cost Analysis groups. All are located in Washington, D.C.

Finally, 20 Navy Commanding Officers/Executive Officers from as many organizations in the fleet volunteered to complete a questionnaire at a Naval Postgraduate School safety class subsequent to an hour lecture by the author. The

lecture described broad system safety concepts and provided some safety definitions.

All interviews began with an explanation of the nature of the research. The interviews were not formalized but were tailored to the interviewee. They were intended to provide the author with candid, uninhibited opinions regarding the conduct of DOD, particularly NAVAIRSYSCOM, system safety activity. Accordingly, interviewees were advised that neither their names nor their respective companies would be linked with individual comments.

II. SYSTEM SAFETY

A. GENERAL

All of the services, of course, want to achieve the same safety objective, i.e., to consciously preclude accidents from happening, and/or to diminish their frequency of occurrence through some deliberate effort.

A technology exists which when exercised makes it possible to achieve this objective. This technology was initially developed by Bell Telephone Laboratories in the early 1960's in response to safety requirements imposed on the "Minuteman" project by the Air Force Systems Command. If one could imagine a recipe which would require one to:

1. Collect data developed under the same contract award from the other "ilities" such as Quality, Maintainability, Value Engineering, Survivability, etc.

2. Review historical accident and failure data available from safety centers, and field and other banks.

3. Emulate the technical and documentational techniques developed for the reliability discipline. To this add a probability of occurrence judgement and severity description assuming an accident will occur.

4. Manipulate all of the above beginning with the system's concept phase and withdraw all action upon systems disposal.

5. Make appropriate hardware and/or operational changes.

The above constitutes the basic ingredient of a safety program. All are described in more detail in "The Safety Standard," MIL-STD-882, System Safety Program for Systems and Associated Subsystems and Equipment.

1. Phases of Acquisition Process

One of MIL-STD-882 requirements is that a safety program should commence as early as possible in the acquisition process. If the above "recipe" were to be properly followed during the concept or development phases of a major weapon system, the end product would be a list of identified hazards pronounced against production hardware which is yet to be built. At worst, the hazards would be pronounced against hardware still in prototype phases. The obvious advantage is that time is available to make low-cost drawing paper changes now rather than expensive ECP (Engineering Change Proposal) production changes or retrofit changes later. Figure 2 is a sample of one such hazard.

2. End Product of Safety Program

Figure 2 represents one F-14 aircraft hazard discovered by the prime contractor's safety organization. It was delivered among others as part of a quarterly delivery from the contractor to the government for bilateral consideration between the government and contractor project management. Briefly, Figure 2 describes catastrophic hazard number 124 found by a contractor safety engineer performing an OHA (Operational Hazard Analysis) in accordance with MIL-STD-882 and the requirements of the development contract. This analysis was performed several weeks before a prototype, live missile firing test was to take place. It was determined by the safety analyst that if the test were to have taken place, the pilot would have exploded his own aircraft.

SAFETY SUMMARY AND STATUS

SUBJECT: AIM-7 PLUME INPINGMENT ITEM NO: 123

SUBMITTED: 6-26-72 BY: J. NIBERT CRITICALITY: IV

HAZ. STATUS: 10-12/0 ACTION REQ'D BY: GAC

DATE CLOSED: TECH. PUBS. AFFECT: YES/NO

PROBLEM SUMMARY:

FUSELAGE LAUNCHED AIM-7 SPARROW MISSILE EXHAUST PLUME MAY PRODUCE SEVERE OVER PRESSURE AND/OR AUTO-IGNITION TO AIRCRAFT FUEL SYSTEM. INITIAL STUDIES REVEAL 67 CUBIC FEET OF MISSILE EXHAUST GAS CAN FLOW INTO THE VENT SYSTEM DURING THE PROJECTED 250 MILLISECONDS OF EXPOSURE THAT WILL BE EXPERIENCED DURING THE MISSILE BURN SEQUENCE.

RECOMMENDED CORRECTION ACTION

RELOCATE FUEL SYSTEM RAM AIR INLET INTO A MORE SUITABLE LOCATION

PROJECT ACTION

o THE FUEL SYSTEM RAM AIR INLET WILL BE REPOSITIONED TO THE TOP FUSELAGE ON A/C #6 FOR ALL FIRINGS FROM CHANNEL STATIONS 3, 4, 5 AND 6. SPECIFIC LOCATION OF INLET TO BE DETERMINED FROM FLOW AND FLIGHT TEST DATA.

o A SERIES OF GROUND TEST FIRINGS UTILIZING AN AIM-7 MOTOR DIRECTED AT A TEST F-14 FUEL VENT MOCKUP WERE CONDUCTED AT CALVERTON IN FEBRUARY 1973.

o FLIGHT TESTS CONDUCTED AT PT. MUGU APRIL-MAY 1973, BOTH LOW AND HI Q, WITH MODIFIED VENT SYS. SHOW SATISFACTORY RESULTS FROM SPARROW STATION 5. TESTS ARE CONTINUING TO WORST CASE CONDITIONS ON STATION 4.

FIGURE 2

An erroneous missile fly-off trajectory was assumed by an aircraft designer in locating the fuel vent. The missile plume would have ignited the fuel system through the mis-located fuel vent.

3. Results and Purpose of Safety Program

In exercising his development contract, a contractor normally performs such tasks as reliability, maintainability, quality assurance, survivability, human factors, etc. It is possible that each of these disciplines may find hazards as chance by-products of their efforts, or they may not. Figure 2, potential hazard no. 123, for example, represents a condition where the vent system was of reliable design, it was maintainable, and of quality construction. Yet, a hazard existed.

The express purpose of the System Safety discipline is to focus on safety by choice, not chance. This is done essentially by having skilled safety engineers using specialized analysis techniques analyze each system and subsystem. The entire scenario is considered. The system and its operators (pilots, maintenancemen, repairmen, overhaulers, movers, testers, handlers of every nature, etc.) using anticipated procedures in their respective "real-world" environment are considered. These analyses are done at a point in time, primarily during the development phase, so that action can be taken economically, to counter the hazards so identified.

By the time the F-14 aircraft contract expired 3½ years later, 133 hazards were found. These were hazards designated as either "critical" or "catastrophic." They were delivered as they were discovered in quarterly installments for subsequent project management consideration and decision. Such is the goal of every system safety program, to identify as many potential hazards as possible for resolution before they are introduced to operating forces as intrinsically deficient hardware, or in other cases, as acceptable hardware but with a high potential for being operated improperly.

B. JUSTIFICATION FOR SAFETY PROGRAM

After Icarus plunged into the ocean and lost his life (and his wings) one could rationalize that he was of no loss to the world. After all, Icarus would probably have been the only pilot known to exist in the world at that time; surely an eccentric at best. Icarus' mission was neither destructive nor protective in any sense of the word. The destruction of a few feathers and beeswax represented an inconsequential economic loss.

The first controllable flying machines were constructed in the early 1900's. The pilots were daring soles seeking adventure. Aircraft weights were in the order of hundreds of pounds. Their energy sources consisted primarily of the relatively few gallons of benzine carried aboard. In contrast, today's craft require well-trained, exceptionally

level-headed pilots. Present aircraft weights are in the order of tens to hundreds of thousands of pounds. Energy sources within the aircraft, just to name a few, are hundreds of pounds of fuel, high pressure hydraulic systems, high capacity oxygen systems, 50 to 100 kva electrical systems, high pressure and temperature pneumatic systems, numerous types of explosive and pyrotechnic devices, high temperature operating machinery, high-energy high-speed rotating engines, etc., any malfunction or misuse of which has a potential for catastrophy not existent in early craft.

When Icarus plunged into the ocean, one could conveniently say that no property was damaged (save Icarus and his wings). He didn't damage the ocean. In a very warped sense, one might even say that he had contributed beneficially to it; his body provided nutrients for aquatic life.

Considering the number of high energy sources mentioned above about current aircraft, the same analogy could not be made of today's aircraft accident. Much is left to chance where property or facilities damage is concerned. If a weapon aboard an aircraft were inadvertently launched while flying over open waters, no facilities or property losses would be expected. Given the same conditions aboard a carrier, another disastrous conflagration such as that which occurred on the Carriers Forrestal and Enterprise could be the result. If an airplane fell out of the sky and crashed in an apple orchard, the extent of property damage is limited

to the loss of a few apple trees, a nominal loss. If, however, the same aircraft crashed into an operational hangar, the facilities loss would be astronomical indeed.

At one time early in flight history, the pilot, navigator, bombardier, mechanic, and serviceman among other things associated with a given aircraft was one and the same man. At the other extreme, today, each of these tasks and many more are performed by specialists. Specialists requiring the use of special ground support equipment perform maintenance tasks on radar equipment, on engine and flight control equipment, on communications equipment, on a host of other equipments too numerous to mention; all of which are far more complex than their counterparts were just a few decades ago, if they existed at all.

1. Environment

The environment referred to here is not the aircraft's well known operational environment. Rather, the environmental conditions are those that influence its development, or that impact the aircraft systems existence.

If the system as defined above were such that it was miraculously devoid of any accident potential, for whichever reasons (perfect Human Factors, Maintainability, Reliability, operated by flawless people, etc.), there would be no need to be concerned about such things as:

Crew losses
Aircraft losses
Operational readiness
Fixes, ECP's

Adverse public opinion
Loss of confidence
Pride of ownership
Money
National Prestige
International Prestige

But accidents do happen. One needs not search very far to recall how an accident influenced each of the above:

Air Force - F-111 (production cut)
NASA - Apollo 204 (1 entire crew and trainer capsule lost)
Army - Cheyenne (project scrapped)
Navy - Forrestal (lives lost, aircraft lost, extensive repair)
Industry - Baton Rouge, La. (chlorine seepage from tanks, city evacuated)

Additionally, the DOD clearly recognizes that public pressure and economic climate have a very definite, profound limiting influence upon its budget. Gone are the days of the everflowing money cornucopia and indiscriminate cost-plus-fixed-fee contracts.

2. Complexity of Weapon Systems

The preceding pages attempt to illustrate that today's aircraft have far more and ever increasing energy sources, the faulty or mistimed action of which, have potentially far greater severity on any particular accident; that aircraft are exceedingly complex in relation to designs of those only several years ago; that each aircraft demands much more specialized attention from many more types of people (pilot, maintenance men, logistics, servicemen, navigator, ordnancemen, etc.) than its elder counterpart did. These are some of the dependent variables that skew the indicator to the higher frequency side of the accident scale;

technological skill skews it toward the "safer" side. The net effect, at least for aircraft accident rates, seems to be a stalemate. Despite increased complexity, increasingly frequent manipulations by greater numbers of people; the accident rate, at least for aircraft, over the last decade as shown in Figure 3 is, roughly, a stable one; perhaps increasing slightly over the last few years.

3. Expense of Weapon Systems

In contrast, the costs associated with essentially the same variables have been increasing steadily. Figure 4 is a rough indicator of an aircraft's relative development cost. Any given weapon system produced today is far more expensive, inflation notwithstanding, than its counterpart was just a few decades ago. The cold, hard, unadulterable aircraft statistics, for example, show that, in 1953, when reliable figures were first documented by the NAVSAFECEN, the average cost of an accident to the Navy was about $75,000. The same aircraft accident (not loss) cost figure today is about $2,000,000, with costs going up almost exponentially. The direct cost of aircraft loss due to accidents in the three-year period from 1972 to 1975 was $1,200,000,000 or about $400,000,000 each year. (21)

Fully one-third of these are due to material failures or design deficiencies or both. This represents every bit of $130,000,000 wasted this past fiscal year in Direct aircraft costs only; again, not considering intangible or unavailable costs as lives maimed or lost, other weapon systems losses,

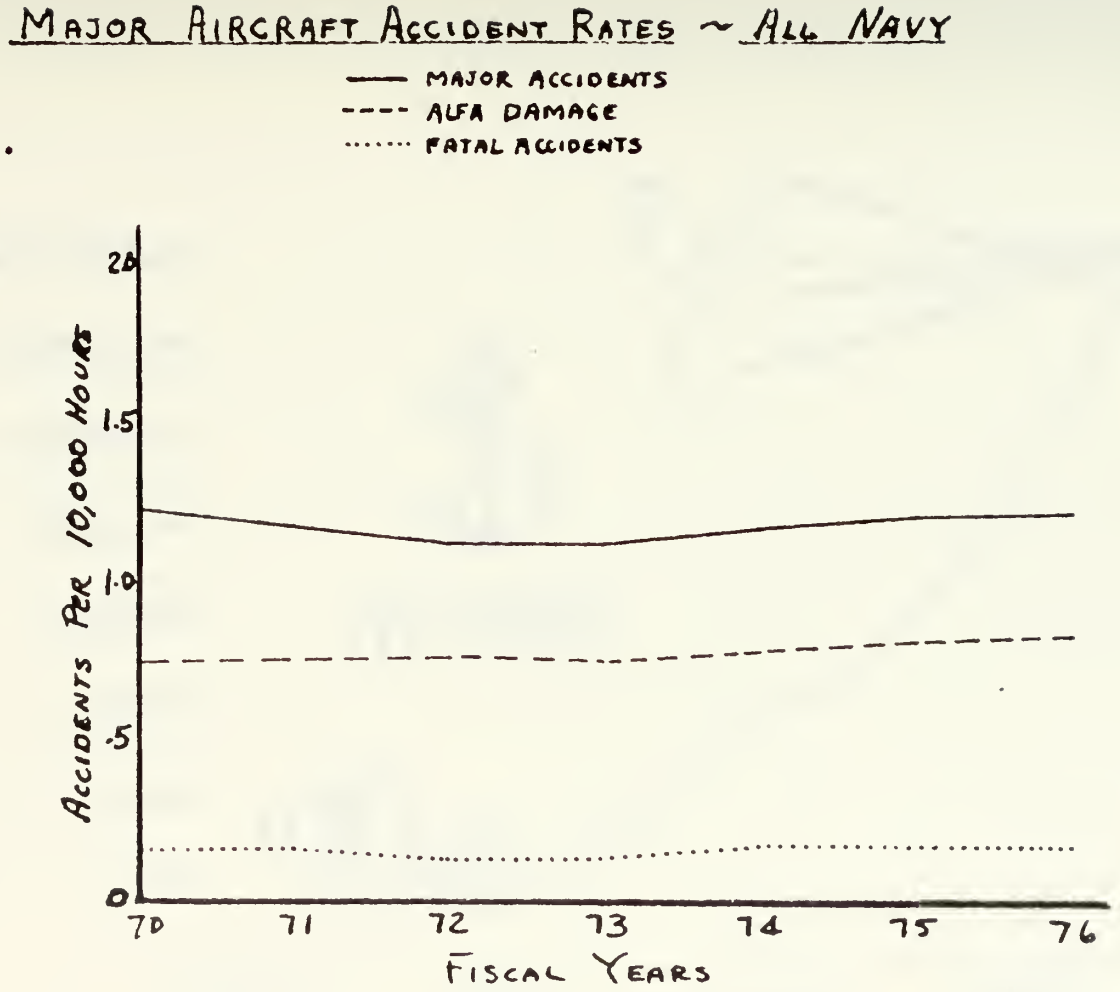
MAJOR AIRCRAFT ACCIDENT RATES ~ ALL NAVY
MAJOR ACCIDENTS
ALFA DAMAGE
FATAL ACCIDENTS
ACCIDENTS PER 10,000 HOURS
2.0
1.5
1.0
.5
0
70
71
72
73
74
75
76
FISCAL YEARS

Figure 3

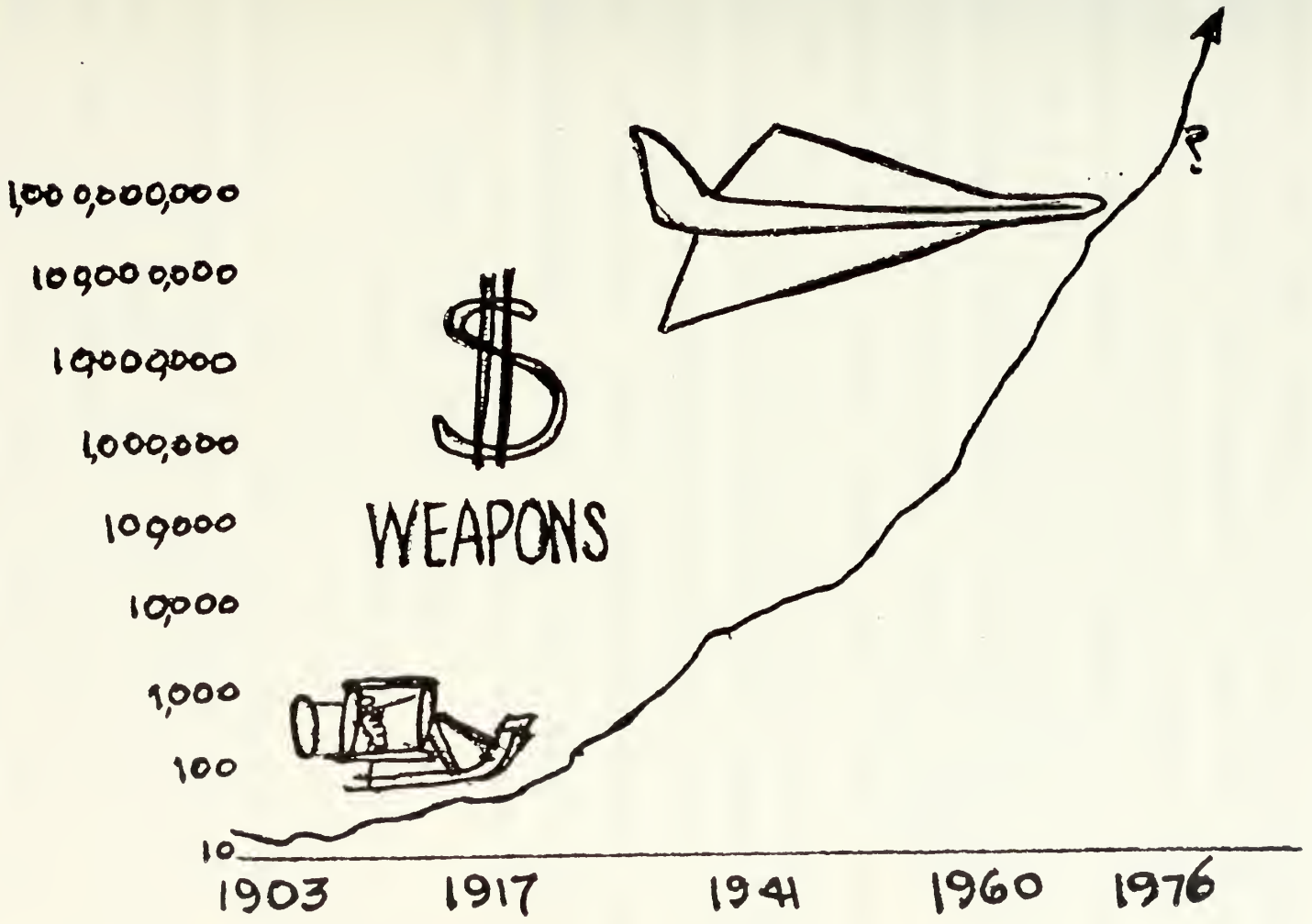

Figure 4.
Aircraft Developmental Costs

other ancillary equipments losses, lawsuit expenses and compensations, court settlement fees, property damages, etc. This incalculable total expense is a very real dollar expense that gets paid for one way or another whether the government can afford it or not. Directly or indirectly, it in some unknown but real proportion reduces the Department of Defense fiscal dollar allocations for research, development, test, evaluation, production, overhaul, maintenance, etc. No project manager would refuse even one 1/100th of the much smaller $130,000,000 portion of the total expense, yet, until within the last decade, virtually no Navy positive preventive actions have been done to reduce these expenses. Most concerted past actions have been corrective measures and have taken place after some dramatic calamity occurs, only to be subdued or forgotten in time.

4. Benefit from a Safety Program

Is there benefit to a safety program? Yes, there is benefit. "How much benefit is there"? one might ask. Unfortunately, no simple answer exists because techniques to measure proceeds from such an effort do not exist. The business of the system safety program is to prevent undesirable events from occurring. How does one determine the costs of what does not happen? Except in a few rare instances, costs computed on the basis of estimates are arguable and indefensible. One rare defensible instance, for the sake of argument, is the event shown in Figure 2, potential hazard No. 123. Clearly, an aircraft costing

$14,000,000 (production estimate) was saved, positively! Perhaps, a pilot or two was also saved. The net benefit is shown below.

Potential Hazard #123
*Direct costs only

	Price of aircraft saved	$14,000,000
	Value of pilot(s) saved	(unknown)
	Resources saved	over $14,000,000
**	Cost of item 123	(560,000)
***	BENEFIT	$13,540,000

Clearly, $13,540,000 represents a real, defensible direct-dollar savings. The benefit was enough to pay for all systems safety programs ever contracted by the NAVAIR-SYSCOM (see Figure 1) and still have monies left over.

More is said on this subject in Chapter II.B.

* Direct dollars only. At the time, early 1972, the congressional mode was to slash defense budgets. Had this potential hazard become a reality, an indirect cost may well have been contract cancellation.

** Cost of finding all 133 hazards, estimate 14 man years @ $20,000/man year and 100% overhead.

*** Benefit from item 123. Benefit from remaining 132 hazards found is incalculable and therefore is not included.

III. INDUSTRY COMMENTS

Informal, unstructured interviews were held with safety members from five major corporations. A number of subjects were discussed, not all of which will appear here. Comments germane to this thesis fell into three broad categories. These are simply listed below. Most will be addressed in subsequent chapters.

A. CONTRACTS

1. Contractors foresee lawsuits regarding safety deficiencies they discover. They can do nothing about them because insufficient dollars are budgeted for Engineering Change Proposals (ECP's).

2. The contractor engineering personnel certification requirements promulgated in MIL-STD-1574, System Safety Program for Space and Missile Systems, are unfair, unjust, restrictive precedent.

3. No research monies are being spent to improve system safety technology.

4. Specific line items should be required in all contracts to perpetuate the safety discipline and to provide administrative stability within contractors' organizations.

B. DATA

1. Too much safety data is requested by the government in the Contract Data Requirements List (CDRL).

2. Statistical accident data provided by the government at request of contractor is woefully deficient.

C. ADMINISTRATION

1. In a contest measuring effectiveness of respective safety programs, the Air Force would be ranked first, the Army second, the Navy last.

2. NAVAIRSYSCOM is grossly deficient in staffing in observable areas such as evaluation of the safety portion of contractor proposals, and in ensuring contractor compliance with the safety requirements of contracts.

3. The Navy Norfolk Safety Center has no clout in contractual safety matters.

4. The Chief of Naval Operations (CNO) and the NAVAIRSYSCOM are at odds with each other concerning cause, disposition of identified operational hazards and/or conditions.

5. Navy safety working groups are transient, lack stability and appropriate expertise in System Safety.

6. Navy safety programs do not involve the government program manager.

IV. THE STATE OF SYSTEM SAFETY IN GOVERNMENT

A. GENERAL

The specification governing System Safety activities is MIL-STD-882, "System Safety Program for Systems and Associated Subsystems Equipment." It was issued 15 July 1969 as a DOD specification superseding MIL-S-38130A, an earlier Air Force safety specification. MIL-STD-882 specifies that it "is mandatory for use by all departments and agencies of the Department of Defense effective 15 July 1969." It further states that:

1. (Par. 1.3.3) the safety life cycle "includes all phases: concept formulation, contract definition (now validation phase) development, production and operation."

2. (Par. 4.2.1.1) for concept phases "A preliminary hazard analysis shall be performed as an integral part of the system concept studies to identify inherent hazards, or risks associated with each design."

Figure 5 illustrates the above-mentioned phases.

B. ECONOMIC ANALYSIS AND OPERATIONAL REQUIREMENTS

1. The Concept Alternatives

When the government wishes to acquire a new weapons system to satisfy a given or newly defined need, it does not arbitrarily procure the first system proposed to satisfy that need. It recognizes that resources are limited, that

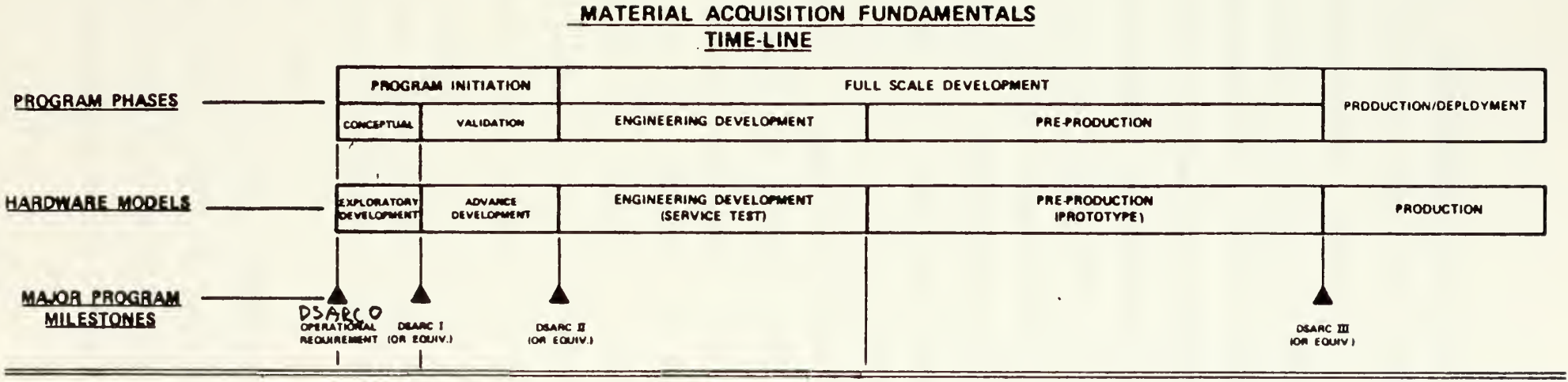
MATERIAL ACQUISITION FUNDAMENTALS
TIME-LINE
PROGRAM PHASES
PROGRAM INITIATION
FULL SCALE DEVELOPMENT
PRODUCTION/DEPLOYMENT
CONCEPTUAL
VALIDATION
ENGINEERING DEVELOPMENT
PRE-PRODUCTION
HARDWARE MODELS
EXPLORATORY DEVELOPMENT
ADVANCE DEVELOPMENT
ENGINEERING DEVELOPMENT (SERVICE TEST)
PRE-PRODUCTION (PROTOTYPE)
PRODUCTION
MAJOR PROGRAM MILESTONES
DSARC 0
OPERATIONAL REQUIREMENT
DSARC I (OR EQUIV.)
DSARC II (OR EQUIV.)
DSARC III (OR EQUIV.)

Figure 5.

once committed, are foregone for other uses, and that it must make its decisions using some rational technique in order to justify expending resources.

The technique advocated by the government is described by DOD Instruction 7041.3, Economic Analysis and Program Evaluation for Resource Management. Under "Policy," this instruction states that whenever resources are to be committed to proposed new projects, an economic analysis "is required." It also states that Project Managers (PM's) should be prepared to demonstrate cost effectiveness of budget proposals. This involves defining the objective, choosing alternatives, formulating assumptions, determining costs and benefits, comparing alternatives, performing uncertainty analysis and finally, making a decision.

To do a cost analysis, all of the resources that are required to achieve meeting the new need or objective are to be shown in the analysis, including all R&D costs, all investment costs and all recurring costs.

Investment costs are costs associated with the acquisition of equipment, all start-up and other one-time investment costs. Recurring or operational costs include personnel, material consumed, operating costs, overhead costs, support costs, etc.

Present Value costs, Economic Life and Inflation considerations are included in these analyses.

Benefits for each alternative are also considered. Finally, an alternative is chosen which either minimizes

costs, assuming benefits/outputs are equal; or maximizes differential output per dollar difference when costs and benefits are unequal.

2. The Operational Requirement (OR)

Ideas for a new weapons system come from a variety of sources. Exploitation of a new technology, recognition of a deficiency, the result of a threat analysis or other studies of prototype programs or military exercises, recognized old-age or obsolescence of current systems, etc. are possible sources which generate ideas. Whatever the source for the idea that results in a need, it must somehow be communicated so that it may be officially recognized and considered for approval. This process begins with the preparation and submission of a document called an "OR," Operational Requirement; the Air Force's and Army's equivalent document is called "ROC" (Required Operational Capability). Again referring to Figure 5, it can be seen that the entire acquisition cycle begins with the OR.

An OR is a three-page document whose purpose is to initiate a conceptual effort to meet an operational need. It briefly describes: (1) the Operational Need; identifies threat parameters, opposition forces, deficiency in present capability, and consequences of not satisfying the operational need; (2) the Operational Concepts: how the system is to be used against the opposition, and (3) the Capabilities Required: performance goals, alternatives, quantities,

cost objectives (design to cost), desired fleet introduction dates, etc.

Draft OR's may be submitted by any fleet activity to a cognizant Force and Mission (F&M) sponsor. The sponsor prepares the OR and controls and monitors its progress throughout the entire acquisition cycle.

OR's are subjected to elaborate reviews. The ultimate goal is approval of the OR by the Secretary of the Navy so that it can be added to the Program Objective Memorandum (POM). The POM contains all of the requirements for all appropriations separated for each of the major mission categories. It represents a part of a long and involved process which takes place to budget for and obtain funds through the Planning, Programming and Budgeting System (PPBS) and the Five-Year Defense Program (FYDP) process (Figure 6), and continues into the fiscal cycle (Figure 7).

If a given subject such as described above, including System Safety is not addressed in the OR, it is not addressed in the POM. If it is not addressed in the POM, it doesn't get funded in the Figure 7 fiscal cycle.

Figures 8 and 9 identify the Navy concept phase acquisition cycle and the documentation and approvals required. The Army and Air Force have a similar cycle.

3. Development Proposal

Once the OR is approved, the CNM is required to respond with a Development Proposal (DP). The DP describes

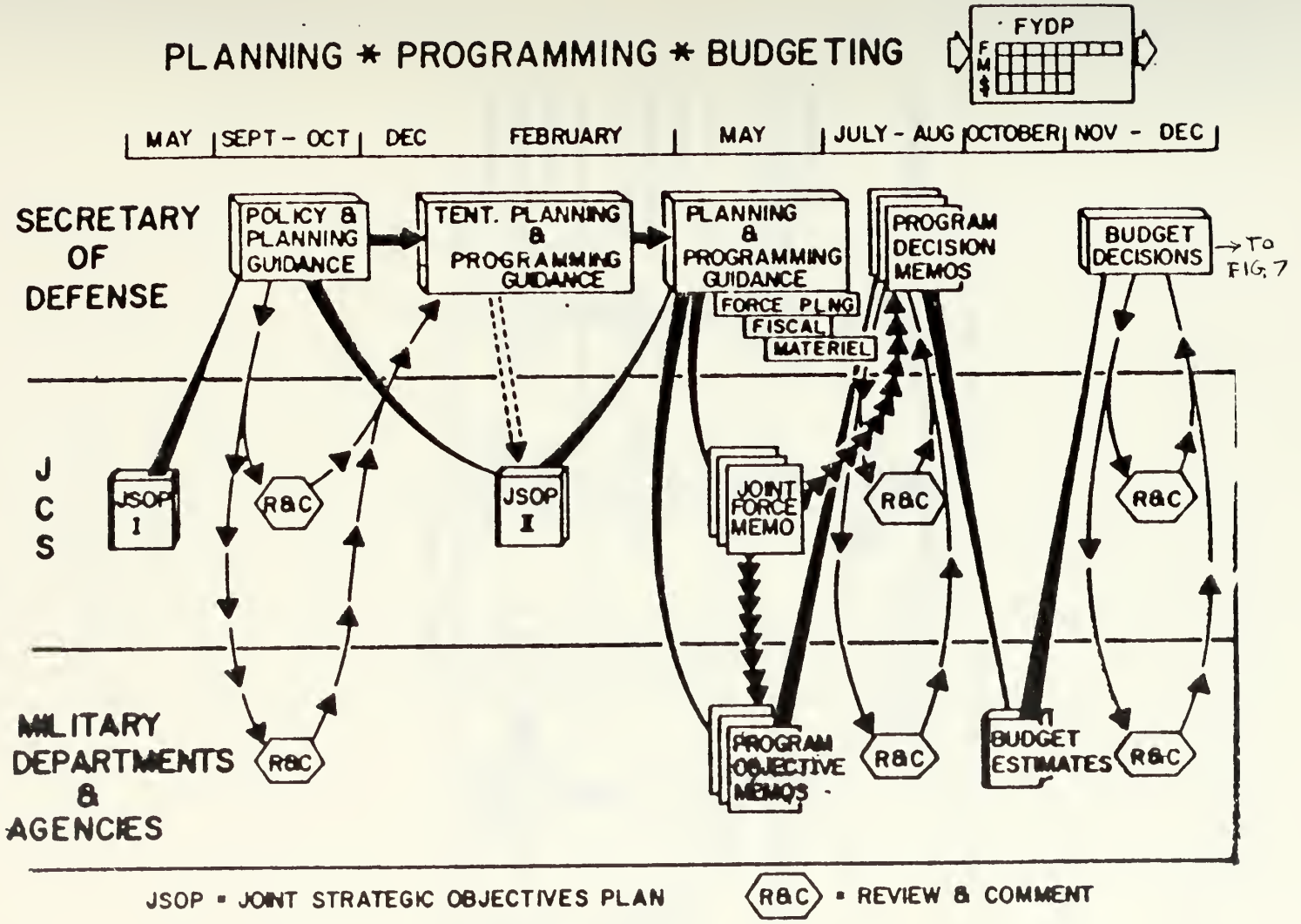
PLANNING * PROGRAMMING * BUDGETING
FYDP
F
M
$
MAY
SEPT - OCT
DEC
FEBRUARY
MAY
JULY - AUG
OCTOBER
NOV - DEC
SECRETARY OF DEFENSE
POLICY & PLANNING GUIDANCE
TENT. PLANNING & PROGRAMMING GUIDANCE
PLANNING & PROGRAMMING GUIDANCE
FORCE PLNG
FISCAL
MATERIEL
PROGRAM DECISION MEMOS
BUDGET DECISIONS
→ To FIG. 7
J C S
JSOP I
R&C
JSOP II
JOINT FORCE MEMO
R&C
R&C
MILITARY DEPARTMENTS & AGENCIES
R&C
PROGRAM OBJECTIVE MEMOS
R&C
BUDGET ESTIMATES
R&C
JSOP = JOINT STRATEGIC OBJECTIVES PLAN
R&C = REVIEW & COMMENT

Figure 6.

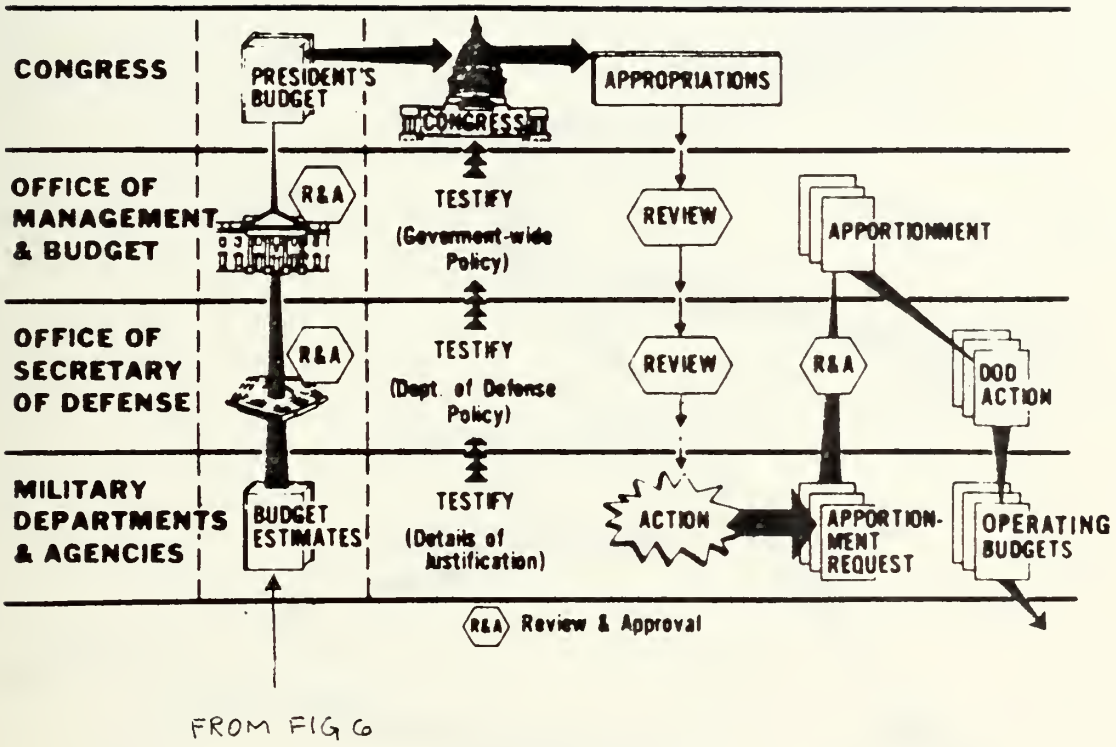

Figure 7.

The Fiscal Cycle

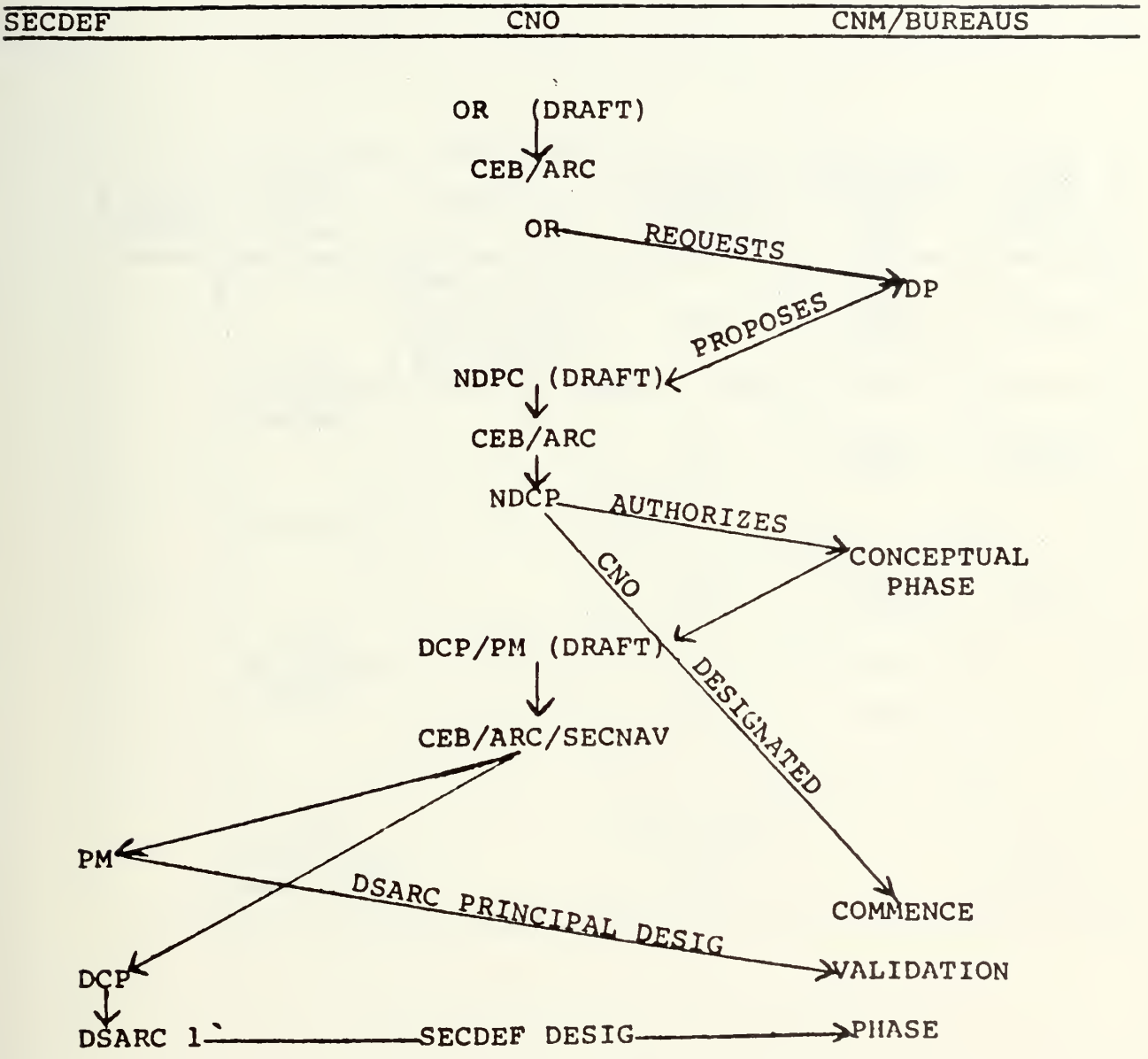

Figure 8.

User-Producer RDT&E Dialogue

BASIC DOCUMENT	TYPE OF SYSTEM	THRESHOLDS 75	DECISION RECORDING DOCUMENT	DECISION REVIEW BODY	LEVEL OF APPROVAL
OR	DOD DESIGNATED MAJOR	$~~50~~ million+ RDT&E and/or $200 million+ Procurement	DCP	DSARC DNSARC CEB/ARC	SECDEF
		As directed	PM	DNSARC CEB/ARC	DSARC PRINCIPAL
	DON DESIGNATED MAJOR		NDCP	DNSARC CEB/ARC	SECNAV
			NDCP	CEB/ARC	CNO
	NON DESIGNATED NON-MAJOR		Abbreviated NDCP		DNPP or DRDT&E

Figure 9.

Navy System Acquisition Operational Requirement Approval Cycle

the technical approach the CNM will adopt to meet the requirements of the OR. Alternative costs and effectiveness comparisons, risks and other detailed back-up information are included within the 20-page proposal. As shown in Figure 9, the DP, then, is approved using either of three recording documents, depending on (a) whether it is designated DOD Major or DOD Non-Major and (b) its dollar threshold.

All three recording instruments, DCP (Decision Coordinating Paper, PM (Program Memorandum) and NDCP (Navy Decision Coordinating Paper) contain essentially the same information to different degrees of elaboration. All three synopsize the elements of the OR.

If a particular subject such as System Safety is not an element in the OR, it is not specifically a consideration in the decisionmaking process leading to an approved DCP and consequently, resources do not follow. The approved DCP represents authority to begin the concept phase.

4. Economic Analysis and Operational Requirements Variances

a. General

If there is to be economic analysis, it should be done early in the concept phase and it should specifically include safety considerations. In evaluating aircraft design alternatives, the analyst should consider such subtle aircraft differences as handling qualities (control response, engine throttle response, etc.), wind loading or other

surrogate criteria. Considering carrier landing operations between several alternatives, for example, such variables as lift coefficient and wing area could have a profound influence on carrier landing accident rates. There are reasons an aircraft such as the A-5 historically has had high accident rates (over 5 major accidents for each 10,000 flying hours) and the A-6 has a much lower rate (less than 2 for each 10,000 hours). An economic safety analysis could conceivably predict such differences.

b. Air Force Policy

The Air Force does perform economic analysis in accordance with a published regulation (AFR 178-1) on subjects such as "Base Closures." It does not do economic analysis on DOD hardware which goes through the DSARC process described above and in Figures 5 and 8. In fact, one regulation specifically forbids analysis of such equipments since "enough analysis is done in the normal acquisition cycle."

c. Army Policy

The Army does do economic analysis at HQ level direction using AR 11-28 as their implementing directive, and ATCD-AD-R Cost and Effectiveness Analysis Handbook (TRADOC Pamphlet 11-8) as a guide.

HQ personnel perform economic analysis concerning non-hardware items such as training centers, installations, bases, etc.

The Combat Development Analysis Office at Fort Monroe, Virginia performs COEA's (Cost and Operations Effectiveness Analysis) for all "DSARC cycle" major and selected non-major projects. The Army has some 80 such projects in being during a given year. About 12 of these projects survive the approval cycle; each includes a COEA.

System Safety is addressed in Army OR's.

d. Navy Policy

Over a half-dozen DOD/SECNAV/OPNAV directives which lead to the preparation of a DCP exist. Only one directive for "Test and Evaluation" specifies that "Safety" should be addressed (in a future TEMP--Test and Evaluation Master Plan).

There is some question about whether or not cost-benefit/economic analyses are being performed anytime during the acquisition cycle by the Navy. Several PMA's indicated economic analyses have <u>not</u> been performed on their respective on-going projects. Several members in the CNM (Chief of Naval Material) OR review cycle indicated economic analysis is <u>not</u> being done. However, a PMA member of the VSTOL-A/CSTOL project indicated that a cost effectiveness analysis will positively be done when alternatives are sufficiently defined. A study to define alternatives is currently taking place; six mission/need variances exist at this time. In any event, a clear policy is not evident.

System safety is not and has not been implemented as directed by implementing instructions into any NAVAIR concept phase projects to date.

Several of the major contractors interviewed were asked if any concept phase contractual efforts performed in the past included System Safety requirements. The answer was "No"!

System Safety has not been addressed in the OR of any NAVAIRSYSCOM project to date.

5. Summary

The Air Force does not perform economic analysis on DOD hardware. The Army does, and system safety is a consideration.

The Army and Air Force consider system safety in the early planning phases. It is given consideration in the Required Operational Capability (ROC--same as Navy OR) and resources follow on approved projects.

The Navy essentially has not performed economic analyses on projects, nor is system safety a consideration in the OR cycle. Safety resources, of course, do not follow.

C. PROJECT OFFICE AND SAFETY OFFICE RESPONSIBILITY

1. The following describes SAMSO (Space and Missile Systems Organization). SAMSO is an equivalent counterpart organization corresponding to the NAVAIRSYSCOM.

a. General

The Safety Office is advised of the existence of a project through receipt of a "Project Directive" (PD) for which they are on automatic distribution. Contact by the Safety Office is subsequently made with respective System

Project Offices (SPO's) and matters dealing with RFP (Request for Proposal) scopes, content, cost, schedule, and data, and in-house administration are determined and exercised in accordance with established policy.

b. Project Manager

Each project manager assigns a full time System Safety representative within his SPO, where feasible. Generally, major SPO's have full time safety representatives; less than major projects have double-hatted representatives as a minimum. Inexperienced safety assignees are required to attend safety courses, usually four weeks at the University of Southern California.

c. Safety Representatives

SPO safety representatives prepare all RFP contractual documentation. They participate in and are responsible for the safety portion in the contractor bid-response evaluation in the contractor source selection process. They are responsible for the conduct of the contractor/government safety program and for contractual compliance assurance after award.

d. System Safety Office

The safety office within SAMSO (and other commands) is essentially a staff office. It establishes safety policy and promulgates it through "regulations" and other documentation. All series regulations dealing with project or contracting functions or which establish

requirements in contracts (Statement of Work, Compliance Documentation, Bidders Instructions, Boiler Plate, Data Requirements Lists and associated Data Item Description, etc.) have been modified to include appropriate system safety program statements. A separate regulation series, a manual, and other guides dealing specifically with System Safety is prepared, published and promulgated. Finally, all MIL-STD's and MIL-SPEC's for which SAMSO is the Office of Primary Responsibility (OPR) are reviewed and safety inclusions inserted where appropriate. All new MIL-SPEC's and MIL-STD's are routed through the office for comment.

The safety office is on automatic distribution to receive all RFP's (about 300 to 400 each year) for approval.

The safety office provides contractual support to the SPO safety representative on a "when requested" basis. Periodic reviews are held with each SPO safety representative; usually once each month, individually and as part of an Inspector General (IG) team, once a year. The staff system safety officer attends SPO contractor/government System Safety Working Group (SSWG) meetings on a spot-check basis to assure compliance with published Air Force system safety policy.

2. Army Responsibility

Lack of funds precluded extensive research. However, it was learned that all regulations pertaining to project functions and to the contract cycle have been reviewed for inclusion of appropriate system safety statements, as was

done by the Air Force. Regulations dealing specifically with System Safety, however, are considered to be insufficient by the Army. Future action at the headquarters level is planned.

This writer is aware that an Army guide exists that explains System Safety in terms of the MIL-STD-882.

3. Navy Responsibility

a. General

The NAVAIRSYSCOM notifies its members of an intent to acquire a new weapon system; as does the Air Force, with a Project Directive. The NAVAIRSYSCOM safety office is not included on the distribution list. The safety office learns of new projects usually through informal channels (hearsay, daily bulletin, notices, newspaper articles, magazines such as Aviation Weekly, rumor, etc.).

b. Project Manager

At this writing, NAVAIR has 23 PMA's (Project Managers, Air) for as many NAVAIR designated weapons systems projects. Each has a charter, a NAVAIR instruction. Each charter identifies an individual by name and designates him to be a "Principal for Safety Matters." The charter further instructs the PMA that he "in collaboration with the Director, Safety Office (AIR-09E) is responsible for ensuring the preparation and execution of an appropriate Naval Air Systems Command safety program for the project." No further instruction regarding safety exists therein.

c. Safety Principal

With one exception, no PMA or PM Safety Principal sought assistance from AIR-09E on his own initiative. With the same exception and one other, all PMA's delegated responsibility to administer safety matters to other organizations. In any event, no Safety Principals nor their delegates received any formal education or training of any kind to perform this function. The business of managing a contractual system safety program is done by a "Class Desk" as a collateral duty in collaboration with the NAVAIR System Safety Office.

No NAVAIRSYSCOM instructions, directives, guides, manuals are available to Safety Principals nor to their delegates, save one short instruction, NAVAIRINST 5100.3A, regarding safety policy and responsibility.

d. System Safety Office

The safety office within the NAVAIRSYSCOM is essentially a staff office. However, as collaborator with all PMA's, the safety office functions as a line organization. Upon learning about the existence of a new weapon system project, the safety officer approaches the Project Manager (PM) to explain the safety program, its purpose, intent, objective, and subsequently negotiates the scope, costs, schedule, and data which are to be included in the proposed RFP.

After award, the safety office arranges contractor/government safety meetings in behalf of the class desk (usually four each year), actively participates in them and

is generally responsible for the conduct of the safety program of all NAVAIR projects.

The safety office is, by NAVAIR instruction, responsible for approving/disapproving all RFP's regarding system safety. The office, however, is not on the RFP distribution list and only approves/disapproves those RFP's which it specifically pursues.

4. Summary

a. Navy and Air Force assign individual safety representatives within respective project offices. Air Force representatives actively pursue safety responsibilities; Navy assignment in the PMA office is essentially perfunctory.

b. Project Directives, RFP's, and MIL-SPEC's and MIL-STD's are automatically distributed to Air Force Safety Offices for review and approval; such distribution is not accomplished in NAVAIR.

c. Army and Air Force have reviewed regulations governing project and contract activity and have inserted appropriate safety requirements. NAVAIR has yet to modify similar instructions.

d. Air Force has provided regulations, guides, manuals, etc., specifically addressing System Safety. The Army has not completed this task but intends to. NAVAIR has not accomplished this task.

D. GOVERNMENT ACCIDENT DATA

1. General

Whenever an aircraft accident occurs, an investigation takes place. Such investigation is conducted in accordance with strict rules, regulations and procedures. All three services perform the investigation in much the same way although there are some subtle differences.

The purpose of an investigation is to ascertain its cause so that action may be taken to preclude its recurrence in another circumstance. In order to foster free, candid expression, witnesses are made aware that any recorded information will be treated with confidentially, and any accident report will be treated as privileged information. Upon completion, the report is filed in a computer.

Contractors have access to "sanitized" reports (no names, no aircraft tail number, etc.) provided they can establish a "need to know" with the appropriate Safety Center. A contract number generally satisfies the need-to-know principal.

2. Safety Center Accident Data

The sanitized data above is useful to contractors. According to the Air Force Safety Center, Norton AFB, full time representatives from 45 major companies receive useful, timely sanitized reports daily on such systems as F-4, T-39, Cruise Missile, etc.

However, almost without exception, the safety personnel interviewed stated emphatically that data from

both the Air Force and Navy Safety Centers in its present deliverable form is next to useless, that data they collect themselves using the same data sources is of more benefit. Bluntly, one contractor, echoing sentiments from the other contractors, said that both Safety Centers are, "a repository for dead data, a statistical graveyard," and that data, when provided, is inadequate in substance and detail, and is untimely.

3. Fleet System Safety Data

It was assumed that Navy operators in the field, being intimately involved with weapons systems, are aware of many potential hazards involved in their use. Further, that if such knowledge were sent to appropriate System Safety Officers, action could be taken to prevent such identified potential hazards from being a reality. A questionnaire completed by twenty fleet Commanding and Executive Officers yielded the following results:

Although 17 of 20 officers heard of OSHA (Occupational Safety and Health Act) and had strong feelings about its implementation in the DOD, only 9 of 20 heard of System Safety and only one of these had any direct involvement.

All were aware of the existence of potential catastrophic hazards having, in their opinion, a high probability of occurring.

Most (12 officers) felt that the current U. R. (Unsatisfactory Report) is a satisfactory reporting system; 6 officers recommended expansion to accommodate system safety; 2 abstained comment.

Only 3 officers felt a "Safety Office" could help.

No U. R. or formal reports of any other nature labeled "Potential Hazard" and request to prevent a potential occurrence have been received by the NAVAIR Safety Office.

4. Summary

a. Safety Center Data, Air Force and Navy (Army--unknown), is unsatisfactory in its present form for system safety engineering use.

b. Fleet personnel have knowledge of existence of potential hazards. Such data transfer, however, does not take place.

c. Most officers never heard of "System Safety."

E. ADMINISTRATION OF SYSTEM SAFETY PROGRAM

1. General

A major system in the development phase progresses from initial ideas, to paper, to prototype hardware system(s) over a long period of time. This phase may last two to five years depending on size and complexity of the system.

It is during this period that the bulk of safety work is most profitably done. All possible potential hazards should be anticipated and predicted at this time.

Typically, a weapon system is an assembly of many subsystems, each of which could be considered as a system by its respective designer. An airplane, for example, is comprised of hundreds of (sub)systems as hydraulic, power, pneumatic, fire control, flight control, communications, air conditioning, etc., etc. As each system being developed is

crystalized, the task of safety personnel is to analyze it, say, the Oxygen System, to determine what possible failure(s) or operational sequence(s) could cause hazards. Production hardware and/or a real-life operational environment is assumed at this time. Having analyzed the Oxygen System, and as the aircraft system progresses, safety personnel analyze the whole airplane as an integrated system to determine if hazardous interfaces exist between (sub)systems. For example, given a safe Oxygen System and a safe Lube System now exist, could it be possible during some future maintenance action to inadvertently interconnect a lube line with an oxygen line with consequent disaster? If so, a potential hazard is reported and dealt with. If not, a potential hazard is reported and dismissed.

During the course of a contractor's safety program, both contractor and government personnel meet periodically to discuss the uncovered potential hazards known to exist at the time. The title given to this group is System Safety Working Group (SSWG).

The health of a safety program is proportional to the intensity of effort expended by the SSWG. The changes effected on the aircraft and/or the changes to future operational procedures both of which were brought about by the hazards found, are a measure of the SSWG success.

2. Air Force SSWG

All members of a project SSWG are chartered and, with a few exceptions, participate in one specific project

only. Membership includes the SPO's assigned safety representative, and individuals having system safety expertise from the Air Force Systems Command, Air Force Logistics Command, the using command, the Air Force's Safety Center, and other DOD and industry organizations as appropriate.

Meetings are held in accordance with the contract schedule. These are generally held just prior to PDR (Preliminary Design Review), prior to CDR (Critical Design Review), and just prior to delivery of data packages affecting explosives safety, nuclear safety or range safety requirements. All members except the SPO safety representative use operational funds to cover travel expenses. The SPO safety representative uses project funds.

The purpose of the SSWG is to discuss only those hazards which the contractor cannot resolve himself because of cost, performance, or schedule constraints. A requirement for membership is authority to make engineering decisions at the SSWG meetings. Members are tasked to resolve hazards brought to their attention at the meeting for presentation at the next meeting. Individual government members also perform safety analysis regarding systems for which they have respective primary interest. "Concerns" found are reported at the next SSWG meeting.

The Norton AFB Safety Center provides safety representation for each project. Here too, with a few exceptions, different members are assigned to different project teams. Again, operational funds cover travel expenses. Depending

on the project, as many as five members from different areas (for example, Flight Safety Division, Life Sciences Division, Analysis Division, Weapons System Division, etc.) participate in a SSWG meeting, each performing his own analysis to find hazards and to supplement the contractor's safety effort. This process continues for the life of the contract.

3. Army SSWG

The Army's administrative style has not been researched due to the lack of funds.

4. Navy SSWG

A formal chartering to identify a given project's SSWG does not exist. Membership generally includes the Class Desk, a member from the safety office, a member or two from the Safety Center, and contractor safety and project personnel. On some funded projects, a member from the safety office from a field activity may attend. The NAVAIR Safety Office member and the Safety Center member attend all other NAVAIR project SSWG meetings.

Meetings are held quarterly in accordance with contract requirements. All members, except the Safety Center member(s), use project money to cover travel expenses, an added expense not felt by Air Force SPO counterparts. All members except the field members employed on a few projects, act as "advisors" to management. They do not routinely perform safety analysis. Field members under work task may perform safety analysis to supplement contractor analysis.

The purpose of the SSWG is to review all critical and catastrophic hazards which were anticipated and discovered by the contractor's safety personnel, whether resolved or not. Additionally, all hazards still left open from previous meetings are also reviewed. All identified potential hazards remain "open" until closing action mutually acceptable to the contractor's management representative and to the class desk is completed. This iterative process continues until contract completion.

The Norfolk, Va. Safety Center provides representation on a select basis. Of the several hundred people employed at the Center, only one individual, a civilian professional engineer, carries the title "System Safety." If there is to be safety representation, it is he who attends practically all projects having Safety Center interest. Some select projects, as the F-14, have an officer assigned to it, in which case two system safety members acting as advisors attend formal SSWG. The Safety Center personnel do not perform formal, scheduled system safety analyses on weapons systems of their interest.

Requests for Safety Center attendance to SSWG meetings are done on an individual basis. Attendance is uncertain because of frequent operational travel fund shortages. In order to offset this condition, several projects have funded the Safety Center, again, an added expense not felt by the Air Force SPO counterpart. In these cases, however, participation and increased membership and support are assumed. On funded

projects, NAVAIR receives on various occasions additional Human Factors, Psychologist, Test Pilot, and Maintenance engineering support.

5. Summary

Air Force's SSWG is chartered, organized. Navy's SSWG is informal.

Air Force SSWG is composed of different members for different projects. Each safety member is a decisionmaker about some area of expertise. Navy safety experts are limited to the same few system safety members. On funded projects, additional support is obtained from the Safety Center and from field activities.

Air Force SSWG members find hazards through analysis, solve specific assigned problems in their areas of expertise. NAVAIR safety members do not perform analyses; act as advisors. Field activities perform safety analyses on funded projects only.

Air Force members consistently have travel expenses covered by operational funds. NAVAIR and NAVAIR field activity members have expenses covered by project funds. The Safety Center uses operational funds but funds are consistently underbudgeted.

V. CONCLUSIONS AND RECOMMENDATIONS

The purpose of this study has been to examine the hypothesis that barriers exist which preclude the utilization of an effective System Safety technology and that these barriers represent a significant barrier to the NAVAIRSYSCOM in particular.

A. CONCLUSIONS

1. A number of significant barriers expressed by contractor as well as government personnel do indeed exist. Some of the problems prevent effective implementation of the safety discipline. All of the below are particularly significant for the NAVAIRSYSCOM.

2. Directives exist which mandate the performance of Systems Safety Requirements in the total acquisition process in accordance with a System Safety Spec. MIL-STD-882.

3. DOD directives and instructions which implement System Safety policies in mainline documentation in both the Fiscal Cycle and the Acquisition Cycle do not exist.

4. Except for one directive (OPNAVINST 3960.10, dealing with a Test and Evaluation Master Plan), all mainline Navy instructions leading to contractual requirements in both concept and development phases of weapons systems acquisition do not specifically address System Safety; Army and Air Force regulations do.

5. Funds to implement "System Safety" specifically are not budgeted for NAVAIRSYSCOM developmental projects in the concept phase.

6. Funds to implement "System Safety" specifically are not bureaucratically, directly budgeted within NAVAIR projects in development phases.

7. Typically, the first request for funds from a NAVAIR Project Manager for system safety expenditures may surface at the time a Purchase Request/Request for Proposal is prepared for an approved weapon system. This occurs long after the planned and approved budget cycle in which case funds for safety are doled in competition with and at the expense of other line items.

8. Economic analyses in accordance with DOD directive 7041.3 are not routinely performed for major projects during the early phases of weapons systems acquisition by the Navy and Air Force. Analyses are routinely performed by the Army. Documentation (instructions, directives, regulations) implementing the above directive is written such that "system safety," specifically is not addressed. "Risk" addressed in the above and other Navy Economic Analysis directives is, by concensus of personnel interviewed, construed to mean "technical" vice "accident" risk.

9. A DOD policy which directs cost-benefit determinations to assess degree of safety among possible weapons systems alternatives does not exist.

10. A DOD policy with descriptive implementing System Safety instruction does not exist.

11. Descriptive NAVAIR System Safety Program documentation (instructions, manuals, guides, etc.) does not exist.

12. The direct safety representation and activity specified in project charters in NAVAIR PMA's exist in name only. Assignments are perfunctory except in the case of two or three projects.

13. NAVAIR's safety office span of control over all projects is so vast as to render the system safety office productivity ineffectual.

14. A viable system safety program saves resources. Just how much is saved cannot be estimated at the present time. Research to determine cost and benefit is needed.

15. NAVSAFECEN policy regarding appointment to and participation in NAVAIR system safety projects does not exist.

16. Data from government safety center banks are completely unsatisfactory in their present form for system safety application.

B. RECOMMENDATIONS

1. DOD Director of Safety Policy: Issue a joint service DOD policy specifically addressing "System Safety."

2. DOD: Direct modification of all mainline acquisition and fiscal cycle directives to include above item 1 policy directive.

3. DOD: Review peripheral documentation such as DOD Directive 7041.3, Economic Analysis. Decide whether the above item 1 policy applies and, of so, direct appropriate changes.

4. DOD: Direct creation of a task force composed of representatives from the three services, NASA, and other agencies to "compare notes" regarding their respective operating procedures, techniques, rules, regulations, etc. Objective: Adoption of most effective issues for improved performance by each organization.

5. DOD/CNO/CNM/SYSCOM's in turn: Determine if system safety is to be a positive force. If so, direct its implementation into mainline documentation. If not, abolish the Safety Standard and all associated documentation.

6. CNO/CNM/SYSCOM's in turn: If above item 4 is determined to be positive, solicit funds independent of project funds, through the fiscal cycle to permit:

a. promotional education.

b. adequate training of full time, dedicated System Safety members.

c. appropriate instruction to all hierarchal levels; SYSCOM line levels, PMA's, CNM/CNO functional levels, CNO sponsors, etc.

d. independent participation in projects.

e. study contracts which could result in:

(1) improved analytic techniques.

(2) better ways to establish project costs.

(3) ways to measure output benefits.

(4) improved data transfer (possibly a common service, DOD Safety Center data bank).

7. NAVAIRSYSCOM Safety Office:

a. solicit NAVAIR funds to:

(1) prepare and publish descriptive system safety guides, manuals and instructions.

(2) have sufficient operating/travel funds to accomplish above publications.

(3) have sufficient operating funds to monitor various safety programs independent of project funds.

(4) adequately train PMA safety principals, and to provide minimal indoctrination for promotional instruction for other NAVAIR hierarchal levels.

b. relinquish line tasks (as prepare RFP verbage, administer individual NAVAIR projects, etc.) and delegate same to assigned PMA Safety Principal. Prepare a NAVAIRINST amplifying the tasks of respective PMA Safety Principals named in project charters.

c. establish, promulgate a clear, specific relationship between NAVAIR and the NAVSAFECEN and other outside safety organizations.

APPENDIX A

C.O./X.O. SAFETY QUESTIONNAIRE

OSHA

1. Have you heard of "OSHA" prior to enrolling in the NPS Executive Safety Course? Yes____ No____

2. (Answer this question only if you are familiar with OSHA policies and objectives) Should OSHA, in your opinion, have relevance to:

a. shore activities? Yes____ No____ don't know____

b. ship activities? Yes____ No____ don't know____

SYSTEM SAFETY

3. Have you heard the term "System Safety" prior to your NPS safety course enrollment? Yes____ No____

a. If yes, what were the circumstances? (Was it a casual or direct involvement? If system hardware [F-14, S3A, AIM9L, etc.] was involved, please identify)_____

_____

_____

_____

4. Considering your operational environment, how many hazards could you conjure within the next two minutes that would fit each of the following (check off as appropriate)

POTENTIAL HAZARDS

Probability of Occurrence	Consequences if occur	Quantity of separate events
a. Low	Low	0____, 1____, 2-4____, over 5____
b. Low	High	0____, 1____, 2-4____, over 5____
c. High	Low	0____, 1____, 2-4____, over 5____
d. High	High	0____, 1____, 2-4____, over 5____

5. a. The existence of a hazard is only one of potentiality; it may not happen.

b. Low probability hazards are not likely to be reported using present communication channels (formal-UR; informal-verbal; telecon and other _____ (fill in).

c. Underlings aware of "potential" hazards will not always choose to reveal them (too trite, censure, too much bother and red tape, too busy, distracted, etc., etc.)
Considering the above, in order to identify potential hazards, are our current communication channels (pick one):

(1) _____ good enough?

(2) _____ should they be expanded?

(3) _____ should they be abandoned in favor of another scheme?

6. Assume that an efficient, acceptable channel to report potential hazards exists. Who, in your opinion, should be the recipient to collect such information, and determine, direct, and control corrective action? (Check off as appropriate)

a. _____ a central DOD agency

b. _____ a central Navy agency

b.1. _____ NAVSAFECEN

b.2. _____ Other (specify)_____

c. _____ Appropriate SYSCOM

c.1. _____ Class Desk

c.2. _____ SYSCOM Safety Office

c.3. _____ Other (specify)_____

d. _____ Other (specify) _____

_____

_____

_____

BIBLIOGRAPHY

1. Hammer, W., Handbook of System and Production Safety, Prentice-Hall, 1972

2. General Dynamics Pomona Division, Fiscal and Life Cycles of Defense Systems, March 1976, third edition.

3. Department of Defense Directive 5000.1, Major System Acquisitions, 18 January 1977.

4. Department of Defense Directive 5000.2, Major System Acquisition Process, 18 January 1977.

5. Department of Defense Handbook, Defense Economic Analysis Council, Economic Analysis Handbook, 2nd Edition.

6. Department of Defense Instruction 7041.3, Economic Analysis and Program Evaluation for Resource Management, 18 October 1972.

7. Department of Defense Military Standard, MIL-STD-882 (Air Force), System Safety Program for Systems and Associated Subsystems and Equipment; Requirements for, 2 April 1970.

8. Department of the Army, AR 15-14, Systems Acquisition Review Council Procedures, 24 January 1975.

9. Department of the Army, AR 70-1, Army Research, Development, and Acquisition, 1 May 1975.

10. Department of the Army, AR 70-17, System/Program/ Project/Product Management, 11 November 1976.

11. Department of the Army, AR 71-3, User Testing, 8 March 1977.

12. Department of the Army, AR 71-6, Type Classification/ Reclassification of Army Material, 13 July 1973.

13. Department of the Army, AR 385-16, System Safety, 22 September 1976.

14. Department of the Air Force, SAMSO Regulation 127-8, System Safety Engineering, 30 April 1976.

15. Department of the Navy, Naval Education and Training Command, NAVEDTRA 10792-P, Financial Management in the Navy, 1974.

16. Department of the Navy, NAVMATINST 5000.22, Weapon System Selection and Planning, 14 January 1975.

17. Department of the Navy, OPNAV 90P-1D, Programming Manual, 1974.

18. Department of the Navy, OPNAVINST 5000.42A, Weapon System Selection and Planning, 3 March 1976.

19. Department of the Navy, OPNAVINST 5000.46, Decision Coordinating Papers (DCPs), Program Memoranda (PMs) and Navy Decision Coordinating Papers (NDCPs), Preparation and Processing of, 10 March 1976.

20. Naval Air Systems Command, NAVAIRINST 5100.3A, System Safety Policies, Objectives and Responsibilities, undated advance copy (1977).

21. Naval Postgraduate School, NPS-034-1-77, Aviation Safety Programs Report, 1 June 1977.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Chairman, Department of Administrative Sciences Code 54 Naval Postgraduate School Monterey, California 93940	1
4.	Professor J. W. Creighton, Code 54Cf Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	2
5.	Professor L. E. Waldeisen, Code 34Wd Aviation Safety Naval Postgraduate School Monterey, California 93940	1
6.	Raymond Banas 2026 Hanover Street Silver Spring, Maryland 20910	1
7.	Irene Hofer 653 W. Ocean View Drive Camarillo, California 93010	1

Thesis
B2095
c.1

Banas
The state of the science of system safety in the Department of Defense.

75355